MIRGHADERI
SYSTEMS ADVISOR

اصول CIAوامنیت اطلاعات در تجارت الکترونیک

استاد: آقای دکتر میرقادری
دانشجو: عرفان تقی مومن

تعریف امنیت اطلاعات

- امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم های اطلاعاتی از فعالیت های غیرمجاز. این فعالیت ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری،واژه های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاه به اشتباه به جای هم بکار برده می شود.
- اگر چه اینها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت نها وجود داردهای ظریفی بین آنها وجود دارد. این تفاوت ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش های استفاده شده برای حل مسئله ،و موضوعاتی که تمرکز کرکه اند دارد.
- امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، و یا اشکال دیگر،امنیت کامپیوتر در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم کامپیوتری تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می شود

CIA

- یکی از اولین موضوعاتی که اموزش حفاظت اطلاعات را پوشش داده است مثلث CIAمی باشد ، این عبارت مخفف سه کلمه ی زیر می باشد که سه رکن اصلی امنیت اطلاعات برای محافظت در برابر تهدیدات و خطرات امنیتی هستند.

محرمانگی : (Confidentiality)اطلاعات فقط باید برای افراد مربوطه در دسترس باشد

صحت یا تمامیت : (Integrity)اطلاعات باید سالم و بدون دستکاری باشد

صحت یا تمامیت : (Integrity)اطلاعات باید سالم و بدون دستکاری باشد

CIA

- وقتی که بحث حفاظت از اطلاعات پیش می امد مثلث CIAمقداری مبهم است. یک راه حل بسیار ساده تر برای تغییر دیدگاه خود این است که طرز فکر یک هکر را داشته باشیم. هکرها قصد انجام سه کار را با اطلاعات شما دارند :
- 1 افشاگریDisclosure
- 2 تخریبDestruction
- 3 انکار Denial
- که این سه عمل دقیقا مخالف مثلث امنیت CIAهستند.من اینها را با عنوان "مثلث هکرها" میشناسیم.به عنوان یک مدافع باید به اصول حفاظت اطلاعات توجه کنیم تا بتوانیم همیشه امنیت را برقرار کنیم. یکی از مهمترین اصول حفاظت این است که آن ها را شناسایی و طبقه بندی کنیم.بسیاری از سازمان ها و ارگان ها قصد دارند از همه اطلاعات خود در یک سطح محافظت کنند ودر این راه با شکست مواجه میشوند. از جنبه های اساسی انها نمیدانند که چه اطلاعاتی برای کسب و کار انها حیاتی است.

CIA

- **افشا سازی**
- افشا سازی مخالف محرمانگی است.شرکت ها باید اطلاعات خود را ارزیابی و انها را دسته بندی کنند. که این عمل به ندرت اتفاق می افتد.کارکنان شرکت ها همیشه باید اگاه باشند تا بتوانند از اطلاعات یک شرکت حفاظت کنند.
- شرکت ها میبایست اطلاعات محرمانه خود را همانند دولت به چند قسمت تقسیم کند و درجه بندی کند :
- ۱ . محرمانه سطح سه:افشا ان ها صدمه جدی به شرکت وارد میکند(تعطیلی ان شرکت)
- ۲. محرمانه سطح دو: افشا ان صدمه قابل توجهی به شرکت وارد میکند(کاهش سهام ان شرکت و اخراج پرسنل)
- ۳. محرمانه سطح یک :افشا ان ایجاد شرمندگی برای شرکت را به همراه دارد(تاثیرات منفی در رسانه ها)
- ۴. عمومی:اطلاعات عمومی
- شرکت ها باید بررسی کنند تا متوجه شوند که چه افشاسازی اطلاعاتی برای انها و مشتریان انها مهم است . سپس انها میتوانند براساس اینکه کدام اطلاعات به بیشترین حفاظت نیاز دارد اولویت هایی برای رفع انها ،سخت تر کردن انها و غیره ایجاد کنند.

CIA

- **تخریب**

- تخریب مخالف بی نقصی است. حالا که شما اطلاعات مهم خود و میزان حیاتی بودن انها را بررسی کردید قادر خواهید بود تا مشخص کنید که چه میشود اگر انها دستکاری شوند یا از بین بروند.سازمان ها باید راه کار هایی برای هر دوی این مشکلات داشته باشند. انها این سوال را باید از خود بپرسند که چه اطلاعاتی بیشتر یک دشمن تمایل دارد نابود کند یا در انها تغییراتی ایجاد کند

- **انکار یا دسترس نبودن**

- انکار یا در دسترس نبودن متضاد دردسترس بودن است .وقتی اسم در دسترس نبودن می اید اولین چیزی که به ذهن شما می اید حملات DDoS حملاتی که باعث داون شدن یک مجموعه میشوند است.حملات DDoSدر موارد زیادی باعث خسارت های قابل توجهی به یک تجارت نمیشوند البته اگر تجارت شما وابسته به فروش انلاین باشد ضربه بیشتری به شما وارد میشود. . نکته در اینجا این است که شما باید شرایط خود را بسنجید.بدیهی است که این یک مشکل است اگر مشتریان شما نتوانند از وب سایتتان استفاده کنند ولی در موارد زیادی لو رفتن یا افشا اطلاعات شخصی انها باعث میشود که دیگر از وب سایت شما استفاده نکنند

تجارت الکترونیکی

- **“تجارت الکترونیک به کلیه فرایند های خرید و فروش، انبارداری، تبادل محصول، خدمات ارائه محصول و فرایند اطلاع رسانی به کمک شبکه های اجتماعی و اینترنت گفته می شود.”**
- یکی از کاربردهای اینترنت، تجارت الکترونیک است. روش های تجارت الکترونیکی باعث رونق و ایجاد شدن کسب کارهای بسیاری در سطح جهان شده است. به شکلی که برای سردمداران این صنعت در آمدهای هنگفتی را به ارمغان آورده است، مانند شرکت Amazonکه درآمد سالانه آن بالغ بر ۲۰۰ میلیارد دلار است.

برنامه جامع امنیت تجارت الکترونیک

- هر ساله سازمان های بسیاری هدف جرائم مرتبط با امنیت اطلاعات، از حملات ویروسی گرفته تا کلاه برداری های تجاری از قبیل سرقت اطلاعات حساس تجاری و اطلاعات محرمانه کارت های اعتباری، قرار می گیرند. چنین حملات امنیتی موجب میلیون ها دلار ضرر و اخلال در فعالیت شرکت ها می شوند
- بی میلی به ارائه اطلاعات مربوط به نقائص امنیتی، از این ترس معمول ناشی می شود که اطلاع عموم از چنین نقائصی باعث بی اعتمادی مشتریان نسبت به توانای ی شرکت در حفظ دارائی های خود می شود و شرکت با این کار مشریان خود و در نتیجه سودهی اش را از دست خواهد داد
- بسیاری از شرکت ها دریافته اند که برای موفقیت در تجارت الک ترونیک، علاوه بر روشهای امنیتی که برای حفاظت از منابع فناوری اطلاعات طراحی شده اند، نیازمند سرمایه گذاری و برنامه ریزی برای ایجاد یک برنامه جامع امنیت هستند تا بدان طریق از داراییهایشان در اینترنت محافظت و از نفوذ مجرمین به سیستم هایشان که موجب خسارت دیدن فعالیت های تجارت الکترونیک شود جلوگیری کنند.

برنامه جامع امنیت تجارت الکترونیک

- برنامه جامع امنیت تجارت الک ترونیک شامل برنامه های حفاظتی که از فناوری های موجود (نرم افزار و سخت افزار)، افراد، برنامه ریزی راهبردی استفاده می کنند و برنامه های مدیریتی که برای حفاظت از منابع و عملیات تجارت الکترونیک شرکت طراحی و اجرا می شوند، است.چنین برنامه ای برای بقاء کلی فعالیت های تجارت الکترونیک شرکت حیاتی است و سازمان باید آنرا به عنوان مولفه اساسی در راهبرد تجارت الکترونیک موفق به حساب آورد.
- موفقیت چنین برنامه ای به حمایت کامل مدیران رده بالا و مشارکت کامل بخش فناوری اطلاعات و مدیریت در جهت درک
- تاثیر گذاری و محدودیت های برنامه است. علاوه بر این برای اطمینان از بروز بودن این برنامه و ابزارهای آن و هماهنگی
- با آخرین فناوری و فنون مدیریت ، باید آن را بطور مداوم مورد ارزیابی و سنجش قرار می گیرد. .

روش های تامین امنیت

- راهکار های امنیت اطلاعات به دو دسته تقسیم می شوند
- **الف) فناوریهای امنیت اطلاعات کنشگرایانه :**انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است
- **امضاهای دیجیتالی:**در دنیای مجازی چطور می توان اطمینان حاصل کرد که پیام ارسال شده است ؟یک راه حل استفاده از امضاهای دیجیتال است که مختص خود فرد است و قابل جعل کردن نیست امضاهای دیجیتال به آنها برای تایید اعتبار فرد فرستنده پیام می شود.
- **شبکه های مجازی خصوصی:** فناوری شبکه های مجازی خصوصی عبور و مرور شبکه را رمز گذاری می کند بنابراین این فناوری برای تضمین صحت و امنیت داده ها به رمز نگاری وابسته است.
- **پروتکل های امنیتی:** شیوه های استانداردکه تبادل اطلاعات رامیان سیستم ها کنترل وهدایت می کنند
- **نرم افزارهای آسیب نما:**برنامه ای برای بررسی نقاط ضعف یک شبکه یا سیستم یاسایت است
- **پویش گرهای ضد** ویروس:برنامه های نرم افزاری هستند که برای بررسی و حذف ویروس های رایانه ای طراحی شده اند کاهای ی که انجام
- می دهند

روش های تامین امنیت

- **ب)فناوریهای امنیت اطلاعات واکنشی:**انجام عکس العمل لازم پس از وقوع یک مشکل خاص امنیتی است
- **دیوار آتش:**اولین خط دفاعی برای دفع مزاحم می باشد دیوار آتش یک فیلتر است که بین سازمان داخلی و اینترنت نصب می شود
- هدف آن جلوگیری از ارتباطات غیر مجاز در درون یا بیرون شبکه داخلی میزبان است.
- **کنترل دسترسی**
- مجموعه سیاست های مربوط به دادن اجازه یا عدم اجازه برای دسترسی یک کاربر خاص به قسمت های مختلف اطلاق می شود
- **کلمات عبور**
- کلمه یا عبارتی است که فرد برای دریافت مجوز دسترسی به اطلاعات باید وارد نماید. زیست سنجی علم سنجش و تحلیل داده های زیستی است . در امنیت اطلاعات از تحلیل ویژگی های بدن انسان مانند اثر انگشت ،قرنیه و شبکیه چشم ،الگوهای صدا،الگوهای چهره و اندامهای دست به منظور تعیین اعتبار استفاده می شود.

تهدیدات و خطرات عمومی شبکه اینترنت

- کپی برداری غیر مجاز و یا سرقت اطلاعات
- ایجاد تغییر و دستکاری در اطلاعات
- انتشار اطلاعات
- تغییر در ساختار ظاهری سایت
- تخریب بانکهای اطلاعاتی
- ارسال و انتشار ویروس

انواع فناوری های حفاظت و ایمنی در تجارت الکترونیک

MIRGHADERI
SYSTEMS ADVISOR

مسیریاب Routers

مسیریاب عبارت از وسیله ای است که مدیریت ترافیک شبکه را انجام می دهد.محلی مناسب برای اعمال قواعد فیلتر کردن بسته ها بر اساس سیاستهای امنیتی هستند.

دیواره آتش Fire wall

سیستم های دیوار آتش آمد و شد به اینترنت را کنترل می کند.

سیستمهای کشف تجاوز IDS

کسی است که بدون اجازه به سیستم شما وارد می شود یا سیستم شما را مورد سوء استفاده قرار می دهد.کلمه سوء استفاده معنای گسترده ای دارد و می تواند شامل دزدی کلان مثل ربودن داده های محرمانه تا استفاده غیر مجاز از پست الک ترونیک شما به منظور ارسال نامه های تبلیغاتی از نوع مزاحمتهای اینترنتی معروف به Spamباشد.

سیستم های کشف تجاوز شبکه ای NIDS

این سیستم ها بسته های داده را که روی کابل شبکه می باشد مورد نظارت قرار می دهند و تشخیص اینکه یک خرابکار مشغول داخل شدن به سیستم است یا خیر یا اینکه سیستم را از ارائه خدمات باز می دارد یا خیر بر عهده دارد.

انواع فناوری های حفاظت و ایمنی در تجارت الکترونیک

تأیید کننده های صحت سیستم SIV

این تایید کننده ها پرونده های سیستمی را به منظور یافتن اینکه چه موقع یک متجاوز آنها را تغییر می دهد نظارت می کنند.

مانیتورهای Log

این سیستم پرونده های Logرا که توسط سرویسهای شبکه ای تولید می شوند مراقبت می کنند.

سیستمهای فریب

این سیستم ها شبیه خدماتی هستند که هدف آنها عبارت از شبیه سازی رخنه های مشهور است تا خرابکارها را به دام بندازد.

امضا دیجیتال

امضاء های دیجیتال، فن آوری دیگری است که توسط رمزنگاری کلید عمومی فعال گردید و این امکان را به مردم می دهد که اسناد و معمالات را طوری امضا کنند که گیرنده بتواند هویت فرستنده را تایید کند.

MIRGHADERI
SYSTEMS ADVISOR

مدیریت را عمیق بیاموزیم...